

UNITED STATES DISTRICT COURT

FILED

SEP 22 2022

for the

Northern District of Oklahoma

Mark C. McCart, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of
 Samsung Galaxy Amp Prime 3, IMEI
 352147100151250, Currently Stored at Homeland
 Security Investigations at 125 W. 15th St., Tulsa,
 Oklahoma 74119

Case No.

22-MJ-599-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

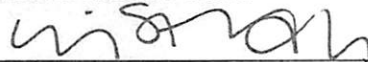
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 1151, 1152, and 2241(c)	Aggravated Sexual Abuse of a Minor in Indian Country
18 U.S.C. §§ 2251(a) and 2251(e)	Production of Child Pornography
18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2)	Possession of or Access with Intent to View Child Pornography

The application is based on these facts:

See Affidavit of Special Agent Erin Staniech, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

Special Agent Erin Staniech, HSI
 Printed name and title

Sworn to before me and signed in my presence.

Date:

9/22/22


 Judge's signature

City and state: Tulsa, Oklahoma

JODI F. JAYNE, U.S. Magistrate Judge
 Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Samsung Galaxy Amp Prime 3, IMEI
352147100151250, Currently Stored at
Homeland Security Investigations at
125 W. 15th St., Tulsa, Oklahoma
74119**

Case No. _____

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Erin Staniech, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent (“SA”) with Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”) since June 2019. I am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child

exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's (FLETC) twelve-week Criminal Investigator Training Program (CITP) and the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252(a), and I am authorized by law to request a search warrant.

4. As part of my duties as an HSI agent, I investigate criminal violations relating to child pornography, including the production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the areas of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child

pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

5. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

6. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 1151, 1152, and 2241(c) (aggravated sex abuse of a minor in Indian country), 18 U.S.C. §§ 2251(a) and 2251(e) (production of child pornography); and 18 U.S.C. §§ 2252(a)(4)(B) & 2252(b)(2) (possession of and access with intent to view child pornography) will be located in the electronically stored information described in Attachment B and is recorded on the Device described in Attachment A.

Jurisdiction

7. “[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.” 18 U.S.C. § 3103a.

8. The requested search is related to the following violations of federal law:

- a. Title 18, United States Code, Section 2241(c) states that “Whoever . . . in the special maritime and territorial jurisdiction of the United States . . . knowingly engages in a sexual act with another person who has not attained the age of 12 years.” For the purposes of that section, a “sexual act” is defined in Title 18, United States Code, Section 2246(2)(B) as “contact between the mouth and the penis, the mouth and the vulva, or the mouth and the anus.
- b. Title 18, United States Code 2251(a) – Production of Child Pornography – is violated by any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.
- c. Title 18, United States Code 2252(a)(4)(B) – Possession of and Access with Intent to View Child Pornography – is violated by any person who knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if—(i)the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii)such visual depiction is of such conduct; shall be punished as provided in subsection (b) of this section.

9. Venue is proper because the person or property described in this affidavit is located within the Northern District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

Identification of the Device to be Examined

10. The property to be searched is a Samsung Galaxy Amp Prime 3, IMEI 352147100151250, hereinafter the "Device." The Device is currently located at Homeland Security Investigations, 125 W. 15th St., Tulsa, Oklahoma 74119.

11. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Definitions

12. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

- a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;

- b. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;
- c. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and
- d. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Probable Cause

13. On or about September 13, 2022, Mayes County Sheriff's Office (MCSO) Deputy Tammy Steddum-Ward, the school resource officer at Locust Grove Middle School, was called to the principal's office. MCSO Deputy Ward was told Eva McDonald, the mother of a student, came to pick up her daughter based on information she received from her son, B.M.

14. Eva notified Deputy Steddum-Ward that B.M. was going through his father's cell phone when he came across disturbing images and a video. B.M.'s father is Billy

Scott MCDONALD. Eva stated her son sent the video to her and asked that she pick him up immediately. I believe B.M. electronically transmitted the video from his father's phone in order to show Eva.

15. Eva stated she watched the video and recognized the voice in the video as MCDONALD.

16. Deputy Steddum-Ward viewed the video and described it as a female child, who appeared to be approximately 2 years old, sucking on a male erect penis.

17. MCSO Investigators and Oklahoma Department of Human Services went to MCDONALD's residence. MCDONALD was not home, however, investigators learned that MCDONALD's residence belonged to his neighbor, Joyce Grisham. Grisham was interviewed and told investigators that she remembered asking MCDONALD to watch her 2-year-old foster child, M.W., while she went to the store approximately three weeks prior to September 13, 2022.

18. M.W. is a member by blood of the Miami Tribe of Oklahoma, a federally recognized tribe. Grisham and MCDONALD live on or near 13563 E 570 Road, Rose, Oklahoma, which is in Indian Country, specifically within the boundaries of the Cherokee Nation. MCDONALD is not an Indian. During a post-Miranda interview with HSI special agents, MCDONALD acknowledged that he is not a member of an Indian tribe.

19. On September 13, 2022, MCSO investigators located and interviewed MCDONALD. Following that interview, MCDONALD was arrested for violations

of Oklahoma State Law. MCSO investigators also seized MCDONALD's cell phone, a Samsung Galaxy Amp Prime 3, IMEI 352147100151250 (the Device).

20. MCDONALD's interview with MCSO investigators resulted in a similar confession to MCDONALD's interview with HSI special agents detailed in the next paragraph.

21. On September 14, 2022, HSI became involved in the investigation. HSI special agent Dustin Carder and I conducted a post-Miranda interview of MCDONALD where he stated at least the following:

- a. That his email address is billymcdonald1975@gmail.com;
- b. That he has had sexual thoughts about children for a very long time;
- c. That he has been able to keep himself away from children so that he does not get himself in trouble;
- d. That he has been living in a building on the same property as Joyce Grisham for approximately three years;
- e. That over the years, Grisham has had approximately three to four foster children stay with her;
- f. That approximately 3 weeks ago, Grisham asked MCDONALD to watch M.W. while she went into town;
- g. At that time, M.W., a two year old female, had only been staying with Grisham for about one day;
- h. That Grisham was gone for approximately 30 minutes and MCDONALD was alone with M.W. during that time;

- i. That he pulled out his erect penis and used his Samsung Galaxy Amp Prime 3 to video M.W. sucking on his penis;
- j. That agents would only find the video of the 2 year old minor female and still shot photos from the video on his cell phone.

22. HSI Special Agents have reason to believe that approximately 20 years ago, MCDONALD sexually abused several of his relatives. The specific nature of that abuse remains under investigation.

23. Based on my training and experience, it is reasonable to believe that MCDONALD has previously attempted to access or successfully accessed child sexual abuse material/child pornography. This belief is based on MCDONALD's statements during his interview that he thought of children sexually for a long time and has avoided children to stay out of trouble, as well as the fact that MCDONALD recorded his sexual abuse of M.W., rather than only sexually abusing M.W.

24. Based on my training and experience, I know that videos and photos can be stored in a variety of locations on cellular phones, including embedded, native, and downloadable applications, and it is impossible to pinpoint the exact location of a video or photo on a cellular phone before searching the phone. I also know that videos and photos can be edited on a cellular phone and copies can be created. Editing or copying a video or photo can change the exchangeable image file format

data (EXIF data)¹ such as the date associated with a video or photo, and therefore, it is impossible to determine an exact date or date range with which to locate the video or photo on the cellular phone.

25. The Device is currently in the lawful possession of HSI. It came into HSI's possession in the following way: Custody of the Device was transferred from Mayes County Sheriff's Office to HSI Special Agent Erin Staniech.

26. The Device is currently in storage at HSI in a locked evidence storage room, located in the Northern District of Oklahoma. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

Technical Terms

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A

¹ Exchangeable image file format data (EXIF data) is the standard that specifies information regarding an image or video each time a new image or video is taken. The EXIF data holds information such as the exposure level, when and where a video or image was taken, type of camera used and any settings used.

wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at

least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic

sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

28. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, a PDA, computer, and allows a user to access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device.

**Characteristics Common to Individuals who
Exhibit a Sexual Interest in Children**

29. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with

whom I have had discussions, I know there are certain characteristics common to individuals who exhibit a sexual interest in children:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media.

Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

- c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically

retain pictures, videos, photographs, correspondence, and mailing lists for many years;

- d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;
- e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;
- f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child

erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

- g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"² it;
- h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of

² See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

individuals with whom they have been in contact and who share the same interests in child pornography;

- i. Such individuals may use social media applications or other means of electronic communications to locate, converse with, and groom minor victims in an attempt to solicit child pornography and/or physically meet and sexually abuse a minor victim;
- j. Such individuals who use social media applications or other means of electronic communications to locate, converse with, and groom minor victims often do not just have one victim. It has been my experience in these types of investigations that such individuals will communicate with multiple victims in an attempt to be more successful in obtaining child pornography and/or physically meeting and abusing a victim
- k. Based on my training and experience, I know that such individuals may use their financial information to buy and sell child pornography online and purchase software used to mask their online activity from law enforcement. For instance, individuals may purchase cryptocurrency such as Bitcoin to buy and sell child pornography online. The use of cryptocurrency provides a level of anonymity because it masks the user's identity when conducting online financial transactions and provides a means of laundering illicit proceeds. Financial information may provide a window into the identities of individuals seeking to buy or sell child pornography online by tying the illicit transactions back to

the user. Financial information contained on an electronic device containing child pornography may also provide indicia of ownership. Further, based on my training and experience, I know that individuals involved in the trafficking of child pornography may use sophisticated software, such as router configuration software, virtual private networks, proxy servers, cryptocurrency exchanges, or other anonymizing software, in conjunction with these illicit financial transactions to provide dual layers of anonymity and prevent law enforcement detection. Financial information may indicate which services were purchased to obscure an individual's identity;

1. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Background on Child Pornography, Computers, the Internet and Email

30. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers, smartphones³ and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;
- b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;
- c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections.

Electronic contact can be made to literally millions of computers and

³ Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

- d. A device known as a router in conjunction with a modem allows numerous computers to connect the Internet and other computers through the use of telephone, cable, or wireless connection. A router, in conjunction with a modem, can connect literally millions of computers around the world. Routers often store information as to which computer used a modem to connect to the Internet at a specific time and location. This information when viewed along with the traces or “footprints” can provide valuable information on who distributed and/or received a visual depiction of a minor engaged in sexually explicit conduct and who possessed and accessed with intent to view a visual depiction of a minor engaged in sexually explicit conduct;
- e. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a

video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

- f. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;
- g. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases; and
- h. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be

intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Electronic Storage and Forensic Analysis

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including production of child pornography and possession of or access with intent to view child pornography, as well as aggravated sexual abuse of a minor in Indian country. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also

know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

33. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like “Whatsapp” and “GroupMe.” Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include production of child pornography and possession of or access with intent to view child pornography, as well as aggravated sexual abuse of a child in Indian country.

34. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of

offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

35. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context,

be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

37. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does

not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

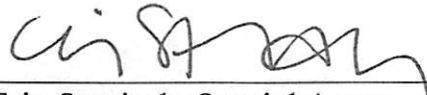
38. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crimes under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

39. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

40. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,



Erin Staniech, Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone on September 22nd, 2022.



JODI F. JAYNE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched is a Samsung Galaxy Amp Prime 3, IMEI 352147100151250, hereinafter the "Device." The Device is currently located at HSI Tulsa 125 W 15th St, Tulsa, Oklahoma 74119.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 1151, 1152, and 2241(c) (Aggravated Sexual Abuse of a Minor in Indian Country); 18 U.S.C. §§ 2251(a) and 2251(e) (Production of Child Pornography); and 18 U.S.C. §§ 2252(a)(4)(B) & 2252(b)(2) (Possession of or Access with Intent to View Child Pornography) involving Billy Scott McDonald, including:

A. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found, including, but not limited to:

1. Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) of child pornography; files relating to the distribution, receipt, or possession of child

pornography, or information pertaining to an interest in child pornography;

2. Files in any form containing the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and
3. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors.

B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution, or production of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were produced, transmitted, or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

1. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by

United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

2. Any and all electronic and/or digital records and/or documents pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;
3. Any and all electronic and/or digital records and/or documents including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;
4. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records,

chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;

5. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;
6. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and
7. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software.

C. Records or other items which evidence ownership, use, or control of the Device described in Attachment A.

D. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access.

E. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educating, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.